NORTH DAKOTA

HOMELAND SECURITY

ANIT-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Furious effort to raise levees in ND town. Crews in Minot, North Dakota, worked furiously June 23 to raise earthen levees in a last-ditch effort to protect some neighborhoods in the town from the rising Souris River, expected to crest June 26 or 27. The effort was focused on protecting critical infrastructure, including sewer and water service, because more evacuations could become necessary if either is knocked out by flooding. The U.S. Army Corps of Engineers drew water down above the Lake Darling Dam so that later releases do not have to be as big. Two shelters opened, one at the city's auditorium and the other at the athletic facility dome at Minot State University, both equipped with water, food, mental health professionals, and nurses. They were nearing the combined capacity of 1,000 by June 22. Source: http://www.msnbc.msn.com/id/43506333/ns/weather/

Higher flood crest to hit Minot; new evacuations. New evacuation orders were issued June 23 in North Dakota, after federal officials said they would dramatically increase the flow of water into the Souris River from a dam upstream on Lake Darling. NBC station KMOT of Minot, North Dakota reported that the Army Corps of Engineers intended to raise the water release from 16,000 cubic feet per second (cfs) to 22,000 cfs by 6 p.m., June 23. Another planned increase on June 24 will bring the flow to 28,000 cfs and will result in a 3 to 4 foot rise in the previously expected river crest. Officials say the water released June 23 night would reach Minot by the evening June 24. More than 10,000 residents fled the city and the area under evacuation orders expanded. Officials announced the closure of the Broadway Bridge, which shut down a key north-south artery in the city. Officials in Burlington, North Dakota, said a new mandatory evacuation was issued. Source: http://www.msnbc.msn.com/id/43506333/ns/weather/

Water on roadway affecting US Highway 52, ND Highway 5 in flooded Souris River basin. Some roads were starting to fall victim to water June 22 in the flooding Souris River basin in north central North Dakota. The state transportation department said the westbound lane of U.S. Highway 52 was closed about 3 miles southeast of Minot because of water on the roadway. The eastbound lane remained open but with reduced speeds. Officials also closed North Dakota Highway 5 about 12 miles west of Mohall because of water. The Souris River was forecast to hit a record level in the Minot area because of excessive spring snowmelt and rain in the basin. Source: http://www.therepublic.com/view/story/7390bbe6325847f6b8b3808689f43be7/ND--North-Dakota-Flooding-Roads/

Dike was damaged in Bismarck while soldiers took cover during storm. Soldiers were pulled off patrol of a dike in Bismark, North Dakota, to take cover during heavy rain and lightning June 18. During that time, a 6-inch pump on the levee clogged, damaging the dike. Crews patched up the area, and the National Guard is confident dikes will hold. Patrolling was back to 24 hours a day by June 19. Source: http://www.wday.com/event/article/id/48090/

REGIONAL

(Minnesota) **Counterfeit bill arrests.** After a 2-month long counterfeit bill investigation, six people in three counties were arrested in Southern Minnesota. During the investigation since May of this year, the Secret Service, Southern Central Drug Investigation unit, and other agencies, have purchased more than $30,000 worth of counterfeit $100 bills. They also collected $3,200 worth of fake bills from businesses. On June 21, an undercover agent talked with one of the suspects to buy $5,000 worth of counterfeit currency. The suspect's husband then showed up with $5,400 worth of counterfeit $100's to sell to the agent, and he was put under arrest. Within a few minutes, search warrants were executed in the cities of Albert Lea, Owatonna, and Faribault. During a search, officers also found money making equipment, methamphetamine, and meth paraphernalia items. Source: http://www.kimt.com/content/localnews/story/Counterfeit-Bill-Arrests/7rmTOpd0ok-Nb0G82NyclA.cspx

(Nebraska; South Dakota; Montana) **Corps to up releases to 160,000 cfs.** Due to heavy rains in Nebraska and South Dakota, the U.S. Army Corps of Engineers announced June 22 that releases at Gavins Point Dam in South Dakota will be increased to 160,000 cubic feet per second (cfs) by June 23. The flows will be increased from 150,000 cfs to 155,000 cfs June 22. and at 8 a.m. June 23, another 5,000 cfs increment will take releases to the 160,000 cfs target. Releases at Gavins Point will remain at that level through August. Releases from Fort Peck in Montana and Garrison in North Dakota will remain at 60,000 cfs and 150,000 cfs, respectively, for the time being. Source: http://www.yankton.net/articles/2011/06/22/community/doc4e016d6b806a5813690633.txt

(South Dakota) **Fort Randall flood makes history.** All four steel flood tunnels opened for a few hours at the Fort Randall Dam near Pickstown, South Dakota June 23. U.S. Army Corps of Engineers officials said for 2011 they maxed out what the power plant could handle and they could not use the spillway because of repairs, so water moved to the tunnels. They said it is not uncommon to use the tunnels during the routine repairs of the spillway, but the amount of water being released s making history. The tunnels release 110,000 cubic feet per second (cfs); the largest release to date happened over 10 years ago with 67,000 cfs. The rest of the week of June 20, the dam will release 138,000 cfs distributed between the powerhouse and spillway. The Corps plans to increase the release to 157,000 cfs the week of June 27. Source: http://www.kdlt.com/index.php?option=com_content&task=view&id=10178&Itemid=57

(South Dakota) **Corps bumps up releases at Oahe Dam at Pierre.** The U.S. Army Corps of Engineers announced it would raise releases at the Oahe Dam in Pierre, South Dakota, another 10,000 cubic feet per second (cfs) the weekend of June 18 and 19, bringing it up to 160,000 cfs by June 19. "We are transferring flood storage from Oahe and Big Bend to Fort Randall, which has more storage available at this time," said the chief of water management for the Corps' northwestern division. "The amount of rain has nearly filled the reservoirs, doing away with most of the flexibility we had built into our operations for this year," he said. The additional volume will be stored at Fort Randall, with the releases at Fort Randall and Gavins Point

remaining at 150,000 cfs. Flows from the Fort Peck and Garrison dams will remain the same, based on current forecast, at 65,000 cfs and 150,000 cfs, respectively. Source: http://www.ktiv.com/story/14933183/corps-bumps-up-releases-at-oahe-dam-at-pierre

National

(Washington) **Justice Dept.: 2 men arrested in plot to attack military recruiting station in Seattle.** Two men intent on attacking a military recruiting station in Seattle, Washington to inspire Muslims to defend their religion from U.S. actions abroad were snared by FBI agents in a terror plot sting, authorities said June 23. A suspect from Seattle, and a suspect from Los Angeles, California, were arrested June 22 after they arrived at a warehouse garage to pick up machine guns to use in the attack, an FBI agent wrote in a criminal complaint filed in U.S. district court. The machine guns had been rendered inoperable by federal agents and posed no risk to the public. The two suspects appeared in federal court in Seattle June 23 and listened as a prosecutor recited the charges against them. Detention hearings were set for June 29. The suspects could face life in prison if convicted. Authorities learned of the plot early in June when a third person recruited to participate alerted the Seattle Police Department, the complaint said. Investigators immediately began monitoring the men, and the confidential informant continued to string them along by promising to obtain weapons. The building, the Military Entrance Processing Station on East Marginal Way in Seattle, also houses a daycare. Recruits for all military branches are screened and processed there. The DHS said in a May 31 assessment with other organizations that it did not think it likely there would be coordinated terrorist attacks against military recruiting and National Guard facilities. Source: http://www.grandforksherald.com/event/apArticle/id/D9O1T5BO2/

U.S. to release oil from strategic reserve. The U.S. Department of Energy (DOE) said it will release 30 million barrels of oil from the Strategic National Reserve to alleviate supply pressures caused by Libyan oil supply disruptions, in the midst of already-plummeting oil prices. The U.S. release is part of a 60 million barrel increase in supply announced June 23 by the International Energy Agency, which includes the U.S. as one of its 28 member nations, “in response to the ongoing disruption of oil supplies from Libya.” The DOE said the reserve is at the “historically high level” of 727 million barrels. “We are taking this action in response to the ongoing loss of crude oil due to supply disruptions in Libya and other countries and their impact on the global economic recovery,” the Energy Secretary said. Source: http://money.cnn.com/2011/06/23/markets/oil_prices/index.htm?hpt=hp_t2 as it pertains to the USA

International

Iran is target of new U.S. sanctions. The U.S. President's administration June 23 imposed new sanctions against Iran Air, Iran’s largest air carrier, accusing it of aiding government organizations that support international terrorism and nuclear proliferation. The new measures

announced by the Treasury Department allege links between Iran Air, the country's national airline, and illegal weapons shipments to terrorist groups in Syria, and also to the transport of high-tech parts for Iran's advanced missiles and nuclear programs. The sanctions restrict U.S. firms from conducting business with the airline in the United States or overseas. Also targeted for sanctions was Tidewater Middle East Co., a major port operator in Iran. U.S. officials said the measures were indirectly aimed at Iran's powerful Islamic Revolutionary Guard Corps, whose leaders are alleged to dominate the country's illicit trade in weapons parts and technology. Iran Air, a commercial airline with a fleet of 40 aircraft serving 25 international cities, has been under a variety of U.S. and international sanctions for more than 15 years. Its jets are banned from many European countries, in part because of concerns about the airline's safety record. Tidewater, which operates in seven Iranian ports and manages a major terminal at the port hub Bander Abas, is owned by the Revolutionary Guard and has been previously accused of using its facilities for illegal shipments. The sanctions are intended to "further expose the [Guard's] central role in Iranian illicit conduct ... so that the international community can take steps to protect against the risk of doing business" with the organization, a senior administration official told reporters in describing the measures at a news conference. Source: http://www.washingtonpost.com/national/national-security/iran-is-target-of-new-us-sanctions/2011/06/23/AGjXO0hH_story.html

Gunmen in Mexico kill 22 as FIFA tournament opens. At least 22 people were killed in a string of attacks in Mexico, authorities said June 19, including a shooting at a bar in Monterrey just hours after the opening of soccer's Under-17 World Cup soccer tournament. Gunmen stormed the bar in Mexico's third largest city late June 18 and "executed three people," wounded another, and kidnapped a security guard at the bar who was later found dead, an official of Nuevo Leon state's investigation agency said. Four other people, 18-25 years old, were killed the morning of June 19 in Guadalupe, a city adjacent to Monterrey. "The victims were gathering in front of one of their homes when armed men showed up in several vehicles and shot them," the official said. Monterrey is one of the host cities for the International Federation of Association Football's Under-17 soccer tournament, and it held two matches on its opening day June 18. The relatively prosperous industrial hub of northern Mexico, home to several foreign companies, was until recently considered a near-safe haven as drug violence increased in many parts of the country. Thirty-three killings were recorded in and around Monterrey, an area of about 4 million people, June 15, making it the area's most violent day in recent history. Another 14 people were killed in the western state of Michoacan, whose bodies were found early June 19, authorities said, also blaming drug cartel-related violence there. Mexico is in the grip of a brutal wave of largely drug-related violence that has killed some 37,000 people since the country's president launched a military crackdown on organized crime in 2006. Source: http://www.google.com/hostednews/afp/article/ALeqM5g0EQDSl09a03RjpSd2V7LykT0bhg?docId=CNG.183747070ebaeb0aaf1c700ebe1075ce.661

Banking and Finance Industry

Banks urged to get faster at reporting cyber breaches. An industry group representing the largest financial institutions said June 21 banks hit by cyber intrusions should immediately notify federal officials and affected customers, amid controversy over Citigroup's decision to wait weeks before informing account holders of a significant breach. The White House recently introduced legislative language that would allow a much longer grace period to inform consumers of data theft. The measure, which is part of a comprehensive proposal to strengthen U.S. network security, would replace a hodgepodge of 47 conflicting state laws with one national requirement to notify people whose personal information has been compromised within 60 days of detecting a breach. Source: http://www.nextgov.com/nextgov/ng_20110621_7982.php

New Zeus emails cloaked as Fed, IRS messages. Small and midsize organizations may want to take note: There is a particularly large Zeus spam campaign making the rounds. The e-mails piggyback on two trusted names — the Federal Reserve and the Internal Revenue Service (IRS) — to incite recipients to take unwise actions. Researchers at Barracuda Labs first spotted the huge uptick in the malicious messages June 20, when the e-mails were blocked before reaching some 120,000 users within 10 minutes. In particular, the e-mails claiming to originate from the Federal Reserve appear to target individuals in charge of an organization's finances. The body of the messages encourage recipients to click on a malicious link for more information about a wire fund transfer that was not processed. Users who click on the link are asked to install an executable, which actually is the data-stealing Zeus trojan, notorious for keylogging the corporate banking credentials belonging to small and midsize businesses, school districts, and charities. On June 22, the fraudsters switched their tactics to leverage the IRS name in their e-mails. The messages contained the same payload, but victims were told their federal tax payment was canceled by their bank, and they were encouraged to click on the malicious link for further details. Source: http://www.scmagazineus.com/new-zeus-emails-cloaked-as-fed-irs-messages/article/205920/

(Illinois) **U.S. sues to seize funds from investor linked to bin Laden.** A key al-Qa'ida member had access to the group's former leader and allegedly financed terrorism invested millions of dollars with a Chicago futures brokerage firm — and now the U.S. government wants to take control of the remaining cash. The man wired $26.7 million into an associate's account in 2005, according to a federal lawsuit by the U.S. Justice Department. The U.S. government froze the accounts in 2007, and is moving to collect the money under federal laws that allow seizure of assets connected to terrorism. While the civil lawsuit does not link the man's money to any terror activity, it portrays him as an al-Qa'ida operative who raised money for the terrorist group and plotted attacks on U.S. citizens and allies. "[The suspect] began raising significant amounts of money through ... a Saudi Arabian-based investment scheme," the lawsuit alleged. "[He] then used the funds raised, in part, to finance jihadist-related activities." He was well connected to al-Qa'ida having met with the group's former leader in 2000 or 2001 in advance of the September 11th attacks on the United States. Source:

http://www.bellinghamherald.com/2011/06/21/2070275/us-sues-to-seize-funds-from-investor.html

Iran scam to evade terror sanctions busted, NYC official says. Eleven companies, including Iran's state-sponsored shipping line, were indicted in New York City June 20 for allegedly conspiring to evade U.S. sanctions on trade with Iran by duping major U.S. banks in order to funnel more than $60 million through the Manhattan banks. The conspiracy indictment seeks to enforce a U.S. ban on trading with Iran that was imposed because the country harbors terrorists and participates in the proliferation of weapons of mass destruction. Iran's national shipping company is alleged to play a key logistical role in that nation's ballistic missile program as well as to serve as a conduit for supplying weapons to terrorist organizations. The Islamic Republic of Iran Shipping Lines (IRISL), its regional offices, and affiliates as well as five individuals were charged in the 319-count indictment with using corporate shells and aliases to "exploit the services of financial institutions located in Manhattan," the district attorney said. According to the indictment, the state-sponsored shipping company allegedly sent or received scores of illegal payments through Manhattan banks by using alias names and corporate alter egos in Singapore, the United Arab Emirates, and the United Kingdom. Among the banks whose security measures were circumvented in the alleged conspiracy were JP Morgan Chase, Standard Chartered Bank, Bank of New York Mellon Corp, HSBC, Deutsche Bank Trust Company Americas, Bank of America, Citibank, and Wachovia (now Wells Fargo), the indictment said. Source: http://abcnews.go.com/Blotter/iran-scam-evade-terror-sanctions-busted-nyc-official/story?id=13885218&singlePage=true

Finance researcher convicted in trade fraud. A finance researcher who prosecutors said used code words like "recipes," ''cooks," and "sugar" to disguise an insider trading scheme was convicted of wire fraud June 20 in federal court. She also was convicted of conspiracy to commit securities fraud and wire fraud in one of the first trials to result from a government crackdown of Wall Street middlemen suspected of peddling inside information as if it were legitimate research. The 43-year-old Fremont, California woman was among 13 people arrested last year on charges she conspired to accept cash and gifts to feed inside information to hedge funds. Most of the other defendants have pleaded guilty. The investigation into Primary Global Research grew out of what prosecutors have called the largest hedge fund insider trading case in history. The main defendant in that case, a one-time billionaire, is awaiting sentencing after being convicted last month for fraud associated with his Galleon Group of hedge funds. Source: http://online.wsj.com/article/APabb11edd14e541cbbb252e26cf1d8bd7.html

Largest Bitcoin exchange offline due to security problems. Activity on Mt.Gox, the largest Bitcoin exchange, was suspended June 20 to deal with two security incidents that led people to doubt the administrators' ability to provide a secure service. Mt. Gox administrators took the Web site offline after a series of large transactions initiated from a compromised account led to Bitcoin prices to plummet. "One account with a lot of coins was compromised and whoever stole it (using a HK based IP to login) first sold all the coins in there, to buy those again just after, and then tried to withdraw the coins. [...]," a Mt. Gox official announced. "Due to the large impact this had on the Bitcoin market, we will rollback every trade which happened since

the big sale, and ensure this account is secure before opening access again. Because the compromised account had a $1,000/day withdraw limit, the hacker didn't manage to steal a large amount. Soon after the incident, a possible source of the compromise surfaced. Apparently, Mt.Gox's entire user database was leaked online. It contains account names and hashed passwords. The exchange has been using freeBSD-style MD5 salted hashing for the past few months, but accounts that haven't been used since the method was introduced still have their passwords in plain MD5. Mt.Gox said it tracked down the source to an auditor who had their computer compromised. The admins extended the downtime to implement a stronger hashing method based on the SHA-512 algorithm with multiple iterations and salting. All users will be forced to update their passwords once service is restored. Mt.Gox also notified Google to ensure every Gmail account listed is locked down and can't be abused. Users who have an account at Mt.Gox are advised to also change their password on any Web site where they might have used it. Source: http://news.softpedia.com/news/Largest-Bitcoin-Exchange-Offline-over-Security-Problems-206958.shtml

Chemical and Hazardous Materials Sector

(Vermont; New Jersey; Illinois) **GAO criticizes NRC's buried pipe regulations, offers recommendations.** The Nuclear Regulatory Commission (NRC) cannot guarantee that underground safety-related pipes can remain structurally sound under its current regulations and standards, according to a report issued by the federal General Accountability Office (GAO). While the NRC believes there is reasonable assurance that the systems will remain structurally sound, stated the report, "(P)ressure and flow tests NRC currently requires do not provide information about the structural integrity of an underground pipe (and) do not indicate the presence of degradation in a pipe that could hinder its future performance." The GAO's two teams of six experts reviewed leaks of tritiated water at Braidwood in Illinois, Oyster Creek in New Jersey, and Vermont Yankee in Vermont, in preparing the report. The Associated Press reported June 21 that tritium has leaked from at least 48 of 65 nuclear sites, according to NRC records. Leaks from at least 37 of those facilities contained concentrations exceeding the federal drinking water standard, up to hundreds of times the limit. The GAO review of the NRC's oversight of underground piping systems was in response to leaks of tritiated water at nuclear reactor sites around the nation. Source: http://www.reformer.com/ci_18326895?source=most_viewed

(Nevada) **U.S. official says Yucca nuclear dump not an option.** A controversial Nevada site is not an option for storing toxic waste from nuclear power plants, a senior U.S. official said. “We do not see Yucca Mountain as a solution here,” the U.S. Deputy Energy Secretary said in an interview June 20. The world has struggled with what to do about nuclear waste for decades, but Japan’s nuclear disaster 3 months ago brought fresh attention to the dilemma as much of the waste is now stored in pools next to reactors. The plan to house atomic waste at Yucca was approved by the then-U.S. President in 2002, but it was opposed by people in Nevada who feared it could pollute water and hurt tourism. The U.S. President’s administration in 2010 asked the Nuclear Regulatory Commission to pull an application to license the dump, and

named a panel of experts to look for other options. But this month, Republican lawmakers said the regulator had found the site suitable for storing nuclear waste, despite administration claims the location was unsafe. Source: http://www.reuters.com/article/2011/06/21/us-nuclear-safety-us-idUSTRE75K0PZ20110621

Commercial Facilities

(West Virginia) **Bomb scare forces evacuation of downtown hotel.** A bomb threat June 24 forced the evacuation of a downtown hotel in Charleston, West Virginia. Kanawha County Metro received a call that a bomb was to go off in the Embassy Suites on Court Street at 7 a.m., a lieutenant with the Charleston Police Department said. Officers quickly responded to the scene and set up a safety perimeter around the hotel while the building was searched, he said. No explosives were found at the scene. However, around 400 people were evacuated from the building while it was searched. The scene was cleared around 8 a.m., and patrons and employees were allowed to return to the building. Area streets were also reopened. The Kanawha County Sheriff's Department brought in the bomb squad to search the hotel. Source: http://www.dailymail.com/policebrfs/201106240093

(Washington) **Home-made bomb detonated outside the downtown library.** What appeared to be a home-made bomb comprised of fireworks was detonated by a bomb squad at 2:12 p.m. June 22 outside the downtown library on Mill Avenue in Renton, Washington. Renton police had evacuated the library about 1 p.m. after library employees found an unidentified “device” in a bag in the bushes near the Cedar River Trail. They called police and the library was evacuated and bomb-disposal specialists were called in. The secured area around the library was enlarged as a bomb-detecting robot prepared to check the bag at about 1:40 p.m. Police closed Mill Avenue South, and the parking lot at the old Renton City Hall building on Mill Avenue was also closed. Mill, the parking lot, and the library reopened shortly after the bomb was detonated. Police and federal agents are conducting an investigation. Source: http://www.seattlepi.com/local/sound/article/Home-made-bomb-detonated-outside-the-downtown-1435946.php

(Utah) **Ogden hostage situation ends with suspect hospitalized.** A hostage situation in Ogden, Utah was resolved the morning of June 18 with the suspect shooting himself and the woman believed to be his hostage released. Ogden police and SWAT teams surrounded a motel at around 5 p.m. June 17 after an armed 37-year-old man refused arrest, and took a hostage. An Ogden police lieutenant said officers were trying to arrest the suspect, a convicted felon and known Nortanos gang member, on a felony drug warrant in front of the the Western Colony Inn at 24th Street where the man had been staying for 10 days. He said the suspect shot at police then ran into one of the rooms and locked the door. Ogden Metro SWAT was called in to assist police. Tenants in the motel were immediately evacuated and a perimeter was set up around the building. The suspect told police over the phone that he was holding a woman hostage inside the room. "The response they got from the suspect was 'no I'm not coming out, you're not taking me voluntarily. Try come taking me, you're going to have a fight on your hands,' " the

lieutenant said. The suspect's family was outside the hotel throughout the standoff, trying to convince him to turn himself in. After hours of attempted negotiations, the SWAT team entered made an explosive entrance to the hotel room to arrest the man at around 9 a.m. The suspect shot himself in the chest, refusing to submit to custody. He was eventually taken into custody and was sent to McKay Dee Hospital, undergoing surgery. His female hostage was unharmed. Source: http://www.fox13now.com/news/kstu-police-man-locked-in-hotel-room-claims-to-have-hostage-20110617,0,5400066.story

(Oregon) **Suspicious device evacuates Salem Center Mall, causes street closures.** A suspicious device at Salem Center Mall in Salem, Oregon evacuated shoppers and closed several surrounding streets the afternoon of June 17, according to local police. The dispatch to police came in at about 3:10 p.m. that a man entered the mall, dropped an orange backpack and left. After a full evacuation, a bomb squad robot determined there was nothing dangerous in the pack. The issue was resolved around 5:15 p.m. The mall sits in the center of downtown, just blocks from several bridges and access to highways. Among the streets closed in the area of the mall: High Street; Union Street; Marion Street; Center Street; and Liberty Street. Several businesses across the street from the mall remained open during the investigation. Source: http://www.koinlocal6.com/news/local/story/Suspicious-device-evacuates-Salem-Center-Mall/EaEaI0jPcUOC02hlYuZtPA.cspx

Communications Sector

Web addresses enter new.era. The organization that regulates the world's Internet domain names approved changes June 20 that could allow anyone to register any name they like in almost any language as a Web address. The new rules affect what the industry calls top-level domain names, the familiar dot-coms and dot-nets that end every Web address. Now, instead of having to use one of those existing forms, users will be able to end their addresses with the name of their company, such as dot-Ford, or their city, like dot-Berlin. If successful, the change could alleviate a shortage of dot-com Web addresses and produce hundreds of millions of dollars in business for the companies whose business is managing the Internet's vast registries, as well as those selling the names, called registrars. Companies could gain new tools for highlighting their identities and networking with suppliers and distributors. The shift, however, could also cause anxiety and disputes among governments, companies and other entities in safeguarding their brands and identities in cyberspace. Those seeking religious or political names, for example, could lead to sensitive situations. Companies, even those that are happy with dot-com and are not interested in adopting a new domain-name suffix, will have to monitor the process to head off any potential trademark or brand-name infringement from other applicants, Internet experts said. Source: http://online.wsj.com/article/SB10001424052702303936704576396963900727284.html?mod=googlenews_wsj

Network Solutions suffers DDoS attack. Network Solutions apparently began suffering a distributed denial of service (DDoS) attack June 20 that left its customers unable to access DNS

servers, hosted Web sites, servers, or e-mail accounts. Reports of outages began appearing late June 20, and by June 21 the company was blaming a DDoS attack. “Some customers may see interruptions caused by a ddos distributed denial of service attack. Our network folks are working on it,” said multiple posts to the Network Solutions Twitter feed the morning of June 21. In a direct response to a customer query June 21, another Network Solutions Twitter message said, “We are dealing with external factors. Your sites are up but dados preventing ppl from reaching. Them”— suggesting a chaotic environment in the support center, as well as the continuing persistence of the DDoS (apparently mistyped as “Dados”) attack. “Network Solutions indicated to us that they had a major DoS attack, which crippled their system, and anyone who has a domain name registered with them,” said the president and CEO and Hospitality Consultants. “The result was that no access to servers or domains was possible for several hours,” beginning at about 6:30 a.m. June 21, EST. Source: http://www.informationweek.com/news/security/attacks/231000095

(Iowa; Nebraska) **Flooding affects cell towers.** Flooding along the Missouri River has prompted AT&T and Sprint Nextel to take a number of cellular towers along the Nebraska-Iowa border offline June 20. Sprint and AT&T eliminated power and service to 12 sites in flooded areas along Interstate 29. Flood levels would damage equipment, including radio and satellite facilities, and the electronics that are stored underground beneath each tower. Sprint built a sandbag fortress and plugged pipes around one of its Omaha, Nebraska wire line switches that powers some of its business land-line customers in the Omaha metropolitan area, and AT&T erected two temporary cell sites in areas not affected by flooding. Two areas affected most by the AT&T outages are I-29 between Pacific Junction, Iowa, and Nebraska City, Nebraska and a patch between Little Sioux and Missouri Valley in Iowa. Source: http://www.omaha.com/article/20110621/MONEY/706219953

Critical Manufacturing

Christmas Tree Shops recall animated safari and aquarium lamps due to fire and shock hazards. Christmas Tree Shops, of Union, New Jersey, issued a recall June 21 for about 35,000 animated safari and aquarium lamps. The lamps were imported by Nantucket Distributing Co. Inc., of Middleboro, Massachusetts. Defective wiring in the lamps can cause an electrical short, posing fire and shock hazards to consumers. Christmas Tree Shops has received three reports of sparking. No injuries or property damage have been reported. The lamps were sold at Christmas Tree Shops stores primarily in the New England, Mid-Atlantic, and Midwest regions from December 2009 through May 2011. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml11/11253.html

MTD recalls TrimmerPlus edger attachments due to laceration hazard. MTD Products Inc, of Cleveland, Ohio, issued a recall June 21 for about 14,500 TrimmerPlus Edger Attachments. The steel shaft that drives the edger blade can break during use causing the edger blade to detach. If the blade detaches, it can hit the user or bystanders, posing a laceration hazard. No incidents or injuries have been reported. The recall involves MTD TrimmerPlus edger attachment model

41AJLE-C092 LE720. The edger is sold separately as an attachment, and can be attached to most major brand attachment-capable trimmers. The edger is used to cut grass along an edge such as a driveway or sidewalk. The TrimmerPlus edger attachments were sold at Lowe's and other hardware and home improvement stores nationwide, and on the Web between March and April. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml11/11252.html

Mazda to recall 400,000 vehicles globally forpossible wiper defect. More than 400,000 Mazda3 and MazdaSpeed3 vehicles worldwide were subject to recall by Mazda Motor Corp. after drivers reported defecwindshield wiper motors. In documents posted June 20 on the National Highway Traffic Safety Administration's Web site, Mazda said it is recalling 103,300 vehiclethe United States manufactured between January 7 and November 28, 2008. The ground terminal of the wiper motor may have been accidentally bent as the cars werassembled, Mazda said in the documents. The flaw may cause the wipers to stop working, which could prove dangerous in inclement weather. Source: http://www.autoweek.com/article/20110620/CARNEWS/110629982

American Samoa confirms evidence of tampering found at shipyard. The American Samoa governor said there were attempts to sabotage the Ronald Reagan Marine Railways shipyard, prior to the government taking back control at the end of May, Radio New Zealand reported June 20. The governor is blaming the former shipyard operator MYD Samoa or others for the attempted sabotage. The vice chair of the authority running the yard for the government confirmed they have found evidence of tampering with equipment that would render it useless for hauling vessels out of the water. The government re-assumed control of the yard after a ruling by a Florida bankruptcy court against MYD Samoa. Source: http://www.rnzi.com/pages/news.php?op=read&id=61300

Defense/ Industry Base Sector

Feds: 2 plead guilty to supplying Iranian military. Two American suppliers pleaded guilty to federal charges of shipping fighter jet and attack helicopter parts to Iranian military officials, and five other people based in France, the United Arab Emirates and Iran are charged with helping, prosecutors revealed June 23. The charges against the overseas individuals were part of an indictment unsealed in Georgia after a man from Macon, Georgia, and a man from Chicago, Illinois, pleaded guilty to conspiring to illegally export the parts to help repair Iran's aging aircraft fleet, prosecutors said. The man from Chicago, an Iranian-born U.S. citizen, was sentenced June 22 to more than 4 years in prison. The man from Macon could face as many as 40 years at his August sentencing. The indictment puts the Macon supplier at the nexus of a complex plot to export military parts for the Bell AH-1 attack helicopter, the UH-1 Huey attack helicopter, and the F-4 and F-5 fighter jets to Iranian military officials through other suppliers in Europe and the Middle East. Source: http://www.stamfordadvocate.com/news/article/Feds-charge-2-with-supplying-Iranian-military-1436962.php

Emergency Services

(Arizona) **Hacker group targets Arizona law enforcement.** The hacker group LulzSec has alarmed police in Arizona the week of June 20 after releasing sensitive information about officers. The group said they posted the information in response to Arizona's controversial immigration law. "We are releasing hundreds of private intelligence bulletins, training manuals, personal email correspondence, names, phone numbers, addresses and passwords belonging to Arizona law enforcement," the group said in a statement. "We are targeting AZDPS (Arizona Department of Public Safety) specifically because we are against SB 1070 and the racial profiling anti-immigrant police state that is Arizona." The Arizona Highway Patrol Association said the release of the documents is unsafe for officers. "Law enforcement officials go to many lengths to protect their identities," stated the president of the organization "These individuals maliciously released confidential information knowing the safety of DPS employees, and their families, would be compromised." Source: http://www.cnn.com/2011/CRIME/06/24/arizona.hackers.documents/index.html?hpt=us_c2

(Ohio) **Northfield police officer finds explosive device on his car, parked at the police station.** An explosive device equivalent to a half stick of dynamite was placed in the wheel well of a Northfield, Ohio police officer's personal car parked behind the police station. The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) is offering a $2,000 reward for information leading to the conviction of the person or persons responsible. The officer saw the illegal device when he walked to his car at 7:40 a.m. June 20 to leave work. The fuse had been lit, but it went out due to the damp, foggy weather that night, the chief said. The ATF, Ohio Bureau of Criminal Identification and Investigation, and the Summit County Bomb Squad responded and are analyzing the evidence. Officers collected pieces of a shattered device and the bottom of a metal container that had been pushed into the ground by the explosion. The container's sides were destroyed. Once the officer found the device on his car, investigators returned to the Coventry Avenue yard and collected more debris and a cigarette butt. Source: http://blog.cleveland.com/metro/2011/06/northfield_police_officer_find.html

Energy

(Pennsylvania) **String of copper wire thefts in Pennsylvania continues.** Pennsylvania authorities are on the lookout for a group of thieves responsible for stealing copper ground wire from several local substations. The latest in the string of thefts occurred at around 4:15 a.m. June 22, when robbers cut out a large piece of barbed wire to gain entrance to a substation near Cranberry, according to the Pittsburgh Post-Gazette. The thieves then cut the copper wire directly from a large transformer, triggering what is known as an arc flash explosion. The explosion crippled the transformer, leaving 3,800 Cranberry-area residents without power for most of June 22. The June 22 incident is one of four copper wire thefts to occur in the Cranberry-area within a week. Copper robberies have become more commonplace in recent months due to the increasing value of the ground wire. Source: http://dark-

fiber.tmcnet.com/topics/dark-fiber/articles/189514-string-copper-wire-thefts-pennsylvania-continues.htm

New rules coming for pipeline control rooms. The U.S. Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA) recently announced that a new regulation to improve the management of pipeline control rooms will go into effect more than a year earlier than originally planned. The final rule will include procedures to improve training, mitigate fatigue, and clearly define roles and responsibilities for employees in control rooms for DOT-regulated pipelines. Control room operators monitor hazardous liquid and natural gas pipelines through computer equipment that records and displays operational information about the pipeline system. Critical functions, such as pressure, flow rates, and valve positions, allow controllers to make informed decisions about what actions to take. These monitoring and control actions are vital to managing pipeline operations along hundreds, and frequently thousands of miles of pipeline. This rule will accelerate pipeline operator requirements by as many as 16 months. These requirements will establish shift lengths and maximum hours-of-service, and develop training programs for control room operators. The action is also a part of the DOT's National Pipeline Safety Action Plan to address immediate concerns in pipeline safety, such as ensuring pipeline operators know the age and condition of their pipelines, proposing new regulations to strengthen reporting and inspection requirements, and making information about pipelines and the safety record of pipeline operators easily accessible to the public. Source: http://ohsonline.com/articles/2011/06/18/new-rules-coming-for-pipeline-control-rooms.aspx?admgarea=news

Pipeline industry influences safety research, regulation. Pipeline operators and their trade organizations shaped, managed and provided sizable funding for many safety studies conducted by the federal agency that regulates the industry, a Hearst Newspapers investigation shows. The studies launched by the federal Pipeline and Hazardous Materials Safety Administration (PHMSA) helped mold national and state safety rules and inspection procedures for 2.3 million miles of pipelines that carry natural gas and hazardous liquids, some underneath neighborhoods. The Hearst Newspapers investigation revealed that two-thirds of the 174 safety studies of land-based pipelines that the federal agency has launched in the last decade were largely funded by pipeline operators or organizations they control. More than half the studies — 89 in total — received funding from five industry trade organizations that conduct research, including three with lobbying arms. Hazards associated with aging pipes — such as defective seam welds that ruptured in the September 2010 natural-gas explosion in San Bruno, California, in which eight people died, and a 2007 propane blast in Carmichael, Mississippi, that killed two people — were the subject of just 5 of the 174 studies the federal agency launched in the past decade. None of those five studies challenged a federal rule that allows pipeline owners to leave such welds in place. A 2004 report said that even current industry practice was too stringent and "likely resulted in the unnecessary repair of numerous seam weld defects." Source: http://www.stamfordadvocate.com/local/article/Pipeline-industry-influences-safety-research-1431183.php

Food and Agriculture

(Washington; Montana) **Livestock disease outbreak in humans probed in 2 states.** Nearly a dozen people in Washington State and Montana who had contact with infected goats were diagnosed with Q fever, a disease common among livestock but rare in humans, state and federal health officials said June 23. The ailment, which can cause fevers and other flu-like symptoms, is the confirmed or suspected cause of illnesses reported in six people in Montana and five more in Washington, where the outbreak began in May. By comparison, Washington typically averages three human cases of Q fever per year, the state department of health spokesman said. Q fever, which is treated with antibiotics, can pose a severe risk to people with heart-valve defects or compromised immune systems. It also can cause pregnant women to miscarry, health experts said. Health and agriculture investigators in Washington have traced the outbreak to a goat herd in the central part of the state where animals on two farms have since been quarantined. The goats from one of the farms were sold to at least one livestock operator in Montana, where three human cases were confirmed and three more suspected, officials said. A spokesman for the Washington Department of Agriculture said animals from the infected herd also were sold in nine other counties in Washington, bringing to 10 the number of counties where local health agencies are on alert for the disease and where livestock inspectors are testing goats. Source: http://www.reuters.com/article/2011/06/24/us-disease-goats-idUSTRE75N0HH20110624

Dole issues precautionary salad recall. Dole Fresh Vegetables voluntarily recalled 2,880 cases of Dole Italian Blend salad that were distributed in the Midwest and eastern United States and three eastern Canadian provinces. There have been no reported illnesses. The precautionary recall was prompted by one package of salad that yielded a positive result for Listeria monocytogenes in a random sample test collected and conducted by the Ohio Department of Agriculture. Source: http://www.thecalifornian.com/article/20110624/NEWS01/106240337

Report: FDA jeopardizes food safety. The U.S. Food and Drug Administration's (FDA) Office of Inspector General (IG) concluded, in a new report, that the FDA has generally failed to promptly initiate recalls, allowed some food companies to continue shipping despite failed inspections and often ignored its own procedures.The study was based on a year-long evaluation of 17 food recalls from 2007 to 2008. The study included a variety of recalls, including those involving cheese, mussel meat, fish, and four separate recalls of fresh cantaloupes from Honduras. The IG's office directed the FDA to review the report as it implements the Food Safety Modernization Act. Development and implementation of food recalls was not adequate to ensure the safety of the U.S. food supply, according to the report, and the FDA often didn't follow its own procedures. Some firms did not promptly initiate recalls, the IG noted. Other problems included weak and inaccurate recall communications from companies conducting recalls, as well as incomplete recall status reports that the firms are supposed to provide the FDA. The FDA failed to conduct inspections or obtain complete information on the contaminated products in 14 out of 17 recalls, the report found. The agency also did not conduct audit checks of consignees in 5 of the 17 recalls, and conducted untimely and incomplete audit checks in the other 12. The agency also failed to review the recall strategy of

firms and promptly issue notification letters to firms covering the review results, the IG noted. Finally, the FDA did not witness the disposal of the products or obtain the required documentation showing that the products were disposed of in 13 of 17 recalls. Source: http://www.thepacker.com/fruit-vegetable-news/Report-FDA-jeopardizes-food-safety-124412499.html

Experts: Seas heading for mass extinctions. Mass extinctions of species in the world's oceans are inevitable if current trends of overfishing, habitat loss, global warming, and pollution continue, a panel of renowned marine scientists warned June 21. The combination of problems suggests there's a brewing worldwide die-off of species that would rival past mass extinctions, the 27 scientists said in a preliminary report presented to the United Nations. Vanishing species — from sea turtles to coral — would upend the ocean's ecosystem. Fish are the main source of protein for a fifth of the world's population, and the seas cycle oxygen and help absorb carbon dioxide, the main greenhouse gas from human activities. "Things seem to be going wrong on several different levels," said the director of global marine programs at the International Union for Conservation of Nature, which helped produce the report with the International Program on the State of the Ocean. Some of the changes affecting the world's seas — which have been warned about individually in the past — are happening faster than the worst case scenarios that were predicted just a few years ago, the report said. Source: http://www.msnbc.msn.com/id/43479398/ns/world_news-world_environment

(Illinois) **Staph found in Illinois bakery tied to outbreak.** Staphyloicoccus aureus (S. aureus) was found inside a Chicago-area cake bakery and in the topping used to finish its cakes, the U.S. Food and Drug Administration (FDA) said in a recently released June 1 warning letter. Rolfs Patisserie of Lincolnwood, Illinois, was implicated in a December 2010 outbreak that sickened 100 people. Many of those who became ill had reported eating desserts at catered holiday parties and at a restaurant. Three of the events had been held in Illinois. Seventy illnesses were reported following a single event in Wisconsin. In connection to that outbreak, Rolf's, which advertises as "a gourmet European Style Bakery" with cakes, pastries, pies, and tarts, recalled all its products, including gingerbread houses sold through Whole Markets in 22 states. Rolfs, which employs about 134 workers temporarily shut down its operations during the investigation to sanitize the bakery. According to the FDA warning letter, S. aureus contamination was found inside the company's 20,000 square-foot facility. FDA inspected the bakery December 23, 2010 through February 23, 2011, taking multiple environmental samples, including those that returned positive for the staph. In the topping material, FDA "confirmed the presence of multiple enterotoxigenic (toxin-producing) strains of s. aureus." The warning letter alleges Rolf's failed to clean and sanitize equipment in a manner that would protect against contamination of food and food-contact surfaces. Source: http://www.foodsafetynews.com/2011/06/staph-contamination-found-in-bakery/

(Wisconsin) **Bacteria that sickened 16 matches Wis. farm's.** Wisconsin health officials apparently have found the source of bacteria that sickened 16 people attending a school event early in June in Raymond. Lab tests show the bacteria that caused the diarrheal illness in people who drank raw milk at the event, matches the strain found in unpasteurized milk produced at a

local farm. Officials said a parent had supplied unpasteurized milk from the farm for the school event. Testing showed the bacteria strain from stool samples submitted by ill students and adults matched the strain from milk samples taken from a bulk tank at the farm. The farm did not sell the unpasteurized milk, and no laws were broken. The farm is licensed and in good standing with the Wisconsin Department of Agriculture, Trade, and Consumer Protection. Source: http://abclocal.go.com/wls/story?section=news/local/wisconsin&id=8198702

Government Sector (including Schools and Universities)

Report: 2,200 IRS databases, including those with taxpayer data, are vulnerable to hackers. Thousands of Internal Revenue Service (IRS) databases that hold sensitive taxpayer information use outdated security software, leaving them vulnerable to hackers, according to a government office that monitors the IRS. The Treasury Inspector General for Tax Administration said that an audit of IRS databases revealed that 2,200 databases the IRS employs to "to manage and process taxpayer data are not configured securely, are running out-of-date software, and no longer receive security patches." The audit, completed in May but released publicly June 23, also said the IRS had not completed its plans to scan its many databases for vulnerabilities. The IRS largely agreed with the report's findings and recommendations, and committed to fixing the issues by December. In a statement June 23, a spokesperson for the agency noted the report made "no direct assertion that any taxpayer data is at risk", and that most of the databases in question do not contain taxpayer data.Source: http://latimesblogs.latimes.com/technology/2011/06/report-2200-irs-databases-including-those-with-taxpayer-data-are-vulnerable-to-hackers.html

(Missouri) **Man infects college PCs to steal huge database.** A former college student has admitted taking part in a criminal scheme that used malware to steal and sell large databases of faculty and alumni, change grades, and siphon funds from other students' accounts. The 21-year-old man pleaded guilty in federal court in Kansas City, Missouri, to computer hacking conspiracy and computer intrusion June 22, according to prosecutors. Charges against his alleged accomplice, a 27-year-old man, are pending, court documents indicated. According to an indictment filed in November 2010, the men developed malware and installed it on the computers of students, faculty, and staff at the University of Central Missouri using many strategies. Ruses included the offer to show vacation photos contained on a thumb drive, and manually installing it on public PCs. The malware contained a backdoor that allowed them to capture passwords used to access restricted parts of the university network, and to spy on computer users through webcams. Prosecutors said the duo managed to install the malware on at least one university administrator's computer, and also succeeded in stealing the login credentials of a residence hall director. Eventually, they used their unauthorized access to conduct fraudulent financial transactions in which they transferred funds into accounts they controlled. They also attempted to sell a database of personal information they stole. Source: http://www.theregister.co.uk/2011/06/23/computer_hacking_guilty_plea/

(Oregon) **Citizen discovers pipe bomb; transports device to city hall.** No one was injured June 17 when a North Plains, Oregon resident found a device that appeared to be a pipe bomb in the parking lot of a local church and transported the device to city hall. At about 2 p.m., the citizen brought the device into city hall. It was then placed in the city hall parking lot and police were called, the city manager said. The North Plains police chief determined the device could be a bomb and the Portland Police Bomb Squad was called. The parking lot was blocked off, and the public and city employees were kept away from the area. The bomb squad arrived and determined the device was made of match heads and a gun powder-type substance. Police placed the device in a metal box and removed it from the parking lot. No one was in danger during the incident. Source: http://www.oregonlive.com/argus/index.ssf/2011/06/citizen_discovers_pipe_bomb_tr.html

LulzSec calls on everyone to attack government assets. LulzSec has launched a new hacking campaign dubbed Operation Anti-Security and calls on everyone, supporters and enemies alike, to attack Web sites belonging to any government agency or government-friendly organization. Judging by the manifesto posted online by the hacking outfit, it seems this effort is in retaliation for the government's attempts to control the Internet. "Our Lulz Lizard battle fleet is now declaring immediate and unremitting war on the freedom-snatching moderators of 2011," the group announced. The hackers said that any online asset belonging to any government is fair game, but notes that banks and other high-ranking organizations are prime targets. Any type of attack was welcomed, such as distributed denial-of-service, Web defacements, and the leaking of classified information. In fact, the latter is described as a top priority. In only a few weeks since its first appearance online, LulzSec has attracted a strong following. It has almost 220,000 followers on Twitter alone, and many of them have demonstrated they have no problem with abusing other people's compromised accounts for fun. Source: http://news.softpedia.com/news/LulzSec-Calls-on-Everyone-to-Hack-Government-Assets-207042.shtml

Information Technology and Telecommunications

Firefox 4 will no longer receive security updates. Mozilla will not provide any more security updates for Firefox 4.0 because 5.0 is considered a replacement and officially starts a new 6-week development cycle. According to a discussion about Firefox 3.6 and 4.0 support on the mozilla.dev.planning mailing list, Firefox 4.0.1 was the only planned update for the 4.0 branch, and it was replaced by Firefox 5.0 when it was release June 21. Mozilla also switched to a silent/automatic update mechanism, but users will be prompted to opt-out if any of their add-ons are not compatible with the new version. Source: http://news.softpedia.com/news/Firefox-4-Will-No-Longer-Receive-Security-Updates-207854.shtml

Malware increasingly being signed with stolen certificates. Cybercriminals are increasingly targeting developers' systems to steal the private keys used to sign software. Programs signed with a digital certificate are considered safer by the operating system and security software,

and the authors of malicious software have caught on. Thousands of certificates have been stolen and are being used by malware, according to the chief technology officer of AVG. In a quarterly security report, AVG found that in the first half of 2011, three times as many certificates were used to sign malware than the first half of 2010. Companies need to better protect their certificates, and security software should become more skeptical of signed code, AVG's CTO said. Source: http://www.darkreading.com/advanced-threats/167901091/security/application-security/231000129/malware-increasingly-being-signed-with-stolen-certificates.html

Feds bust international gangs distributing scareware products. Federal law enforcement authorities working in cooperation with their counterparts in more than 10 countries disrupted the operations of 2 gangs responsible for distributing malicious scareware programs to more than 1 million people. Two Latvian citizens were indicted and more than 40 computers and several bank accounts were seized in connection with the action dubbed Operation Trident Tribunal. The two individuals face up to 20 years in prison if they are convicted on all charges. A statement issued by the FBI June 22 said the two Latvians were arrested June 21 in Rezekne, Latvia, for allegedly distributing and selling nearly $2 million worth of such scareware products. The two were charged with wire fraud, conspiracy to commit wire fraud, and computer fraud. An indictment unsealed in federal court in Minneapolis, Minnesota, accused the two of creating a fake advertising agency, and using it to plant a malicious advertisement in the Minneapolis Star Tribune with the intent of distributing scareware. Source: http://www.computerworld.com/s/article/9217866/Update_Feds_bust_international_gangs_distributing_scareware_products

DNS agility leads to botnet detection. Online criminals have evolved tactics to harden botnets against takedown using many tactics, including fast-flux networks and Conficker-like dynamic domain generation. Yet, such tactics can also pinpoint when such networks are being created by bot operators, according to research from the Georgia Institute of Technology. The research found that dynamically detecting changes in the domain name system (DNS) can lead to the early detection of botnets. When bot masters create the infrastructure for a botnet, the reputation of the domain names can tip off defenders. In two papers, researchers found they can detect anomalies in the domain name system indicative of botnets and have documented recognition rates greater than 98 percent. Network security firm Damballa announced June 20 a service based on the research to provide intelligence on botnet-infected systems. Called FirstAlert, the service can detect the characteristic DNS queries indicative of botnet infections inside a customer's network. Source: http://www.computerworld.com/s/article/9217827/DNS_agility_leads_to_botnet_detection

UK police make arrest in hacking attacks. A 19-year-old man was arrested June 20 in Wickford, England, on suspicion of hacking attacks on Sony and the CIA Web site, British police said June 21. The Metropolitan Police said the arrest took place following a joint operation by its Internet crimes unit and the FBI. Police would not say if the suspect was tied to the Lulz Security hacking collective, which has claimed responsibility for recent high-profile attacks, but did confirm that a computer seized in the operation will be examined for Sony data. Lulz had boasted of

successfully hacking Sony in addition to subsequent attacks on the CIA Web page and the U.S. Senate computer system. The hackers recently called for "war" on governments that control the Internet. The teenager was taken to a central London police station for questioning, police said. Officers are conducting forensic examinations on "a significant amount of material" found in the search of a home following the arrest. Source: http://www.google.com/hostednews/ap/article/ALeqM5gfsex1AN6xkwlkauBQivxe8GgBrQ?docId=06f3b7c8416e43f2888dbc30b0cad1bd

Hackers move fast to exploit just-patched IE bug. Just 3 days after Microsoft patched 11 bugs in Internet Explorer (IE), hackers are exploiting 1 of those vulnerabilities, a security company said June 17. Microsoft fixed the flaw June 14 in an 11-patch update for IE. That update was part of a larger Patch Tuesday roll-out that quashed 34 bugs in 16 separate security bulletins. Most security experts had put the IE update at the top of their priority lists, and urged Windows users to deploy it as soon as possible. Symantec reported June 17 that CVE 2011-1255 — its assigned ID in the Common Vulnerabilities and Exposures database — is already being abused. "So far, we have only seen limited attacks taking advantage of this vulnerability and believe that the exploit is only being carried out in targeted attacks at present," a senior researcher with Symantec's security response team said. He said Symantec found an exploit on a compromised site that automatically downloads an encrypted malicious file to the PC of any user browsing with an unpatched copy of IE8. The malware shows some bot traits, he added. Once planted on a machine, it contacts a remote server and listens for commands from its hacker overlords. Although the CVE 2011-1255 vulnerability affects IE6 and IE7 as well as IE8, Symantec has only seen working exploits that target the latter. Source: http://www.computerworld.com/s/article/9217727/Hackers_move_fast_to_exploit_just_patched_IE_bug

Reports: Sega customer database hacked. Video game company Sega had a database hacked and sensitive information on about 1.3 million customers has been compromised, according to media reports. The database of the Sega Pass Web site includes customer names, dates of birth, e-mail addresses, and encrypted passwords. Various media outlets have been able to confirm the attack with officials from the Japanese company. The news site Playstation Lifestyle posted the text of an e-mail that Sega reportedly sent to Sega Pass registered users June 17 informing them of the breach. In the letter, Sega stresses that passwords were not stored in plain text, but rather encrypted, and that payment information was not involved in the incident. Source: http://www.computerworld.com/s/article/9217747/Reports_Sega_customer_database_hacked

National Monuments and Icons

Wildfires burn 1.4 million acres across 12 states. Firefighters in 12 U.S. states have their hands full with dozens of more wildfires. The Wallow fire in Arizona and New Mexico is one of 53 large uncontained wildfires burning in the United States, from Alaska to Florida, according to the

National Interagency Coordination Center. All told, the fires have burned 2,166 square miles or 1.4 million acres — nearly the size of Delaware. About 10,400 firefighters are involved in efforts to contain the fires, with more than 7,000 of them in Arizona and New Mexico, where fires have burned 853,518 acres, according to the center. The largest of the fires continues to be the Wallow Fire, which has burned 527,774 acres so far, the fire's incident command team announced June 21, and is about 58 percent contained. While residents in Greer, Arizona, are being allowed to return home, evacuation orders remain in effect in other parts of Arizona and in Luna, New Mexico. Residents in parts of Apache County, Arizona, also have been told to be prepared to evacuate should the need arise. In Texas, a fast-moving fire near Grimes County destroyed at least 26 homes as it burned across more than 4,000 acres. The fire was caused by homeowners grilling near Stoneham, Texas, CNN affiliate KHOU-TV reported. In North Carolina, Forest Service officials said they are closely monitoring a fire in Pender County, which has burned more than 4,000 acres. The number of wildfires so far this year is below the 10-year average for the United States, according to the U.S. Forest Service. But the number of acres burned is 3 times that 10-year average, according to the agency. Source: http://www.cnn.com/2011/US/06/22/wildfires/index.html?hpt=hp_t2

(Oregon) **Police raid major pot grow in NE forest.** A multi-agency team arrested six people June 16 at an outdoor marijuana grow operation that was discovered by bear hunters on U.S. Forest Service land in a remote forest area in Enterprise, Oregon. It is believed to be the largest grow operation discovered to date in Oregon. Police said a group of bear hunters came across the site this spring and reported it to local law enforcement. Authorities were assisted by an Oregon State Police SWAT team and air support from the Oregon Army National Guard. Suspects aged 26, 24, 28, 32, 21, and 29 were arrested and lodged at the Union County Jail. All were held on charges of unlawful manufacture and possession of marijuana. A La Grande Police sergeant, who is team supervisor of the Union/Wallowa County Drug Team, described the grow as "staggering," encompassing a stretch over 1 mile in a ravine where growers disrupted the terrain with terracing. Over 91,000 plants ranging in size from starters to larger plants were eradicated over a 2-day period. The plants were concealed in several separate pods developed by removing trees and underbrush to camouflage the grow site, and "miles" of plastic irrigation tubing was also found. Investigators found campsites and numerous weapons, including semi-automatic long barrel firearms and handguns. Food, water, and other supplies were found at campsites that could sustain the growers for several weeks. Source: http://www.bluemountaineagle.com/free/police-raid-major-pot-grow-in-ne-forest/article_7a444486-9914-11e0-a50b-001cc4c03286.html

Postal and Shipping

(Massachusetts) **Mass. man sentenced for ricin, prosecutor threat.** A former Agawam, Massachusetts man has been sentenced to 15 years in federal prison for illegally possessing the toxin ricin, and threatening a prosecutor. The man pleaded guilty to the charges in March. He has been in federal custody since 2004, when he was arrested on charges of using the mail to transport a firearm. Agents who searched his apartment discovered what appeared to be a

weapons lab along with castor and abrus seeds — the sources of ricin and abrin poisons. Prosecutors said he later sent a letter to an assistant U.S. attorney in which he invoked the name of the Oklahoma City bomber. A U.S. district court judge sentenced the 57-year-old man June 20 to the maximum 15 years in prison, followed by 3 years supervised released. Source: http://www.ctpost.com/news/article/Mass-man-sentenced-for-ricin-prosecutor-threat-1432530.php

U.S. postal service shuts door on mail to Canada. The United States Postal Service (USPS) stopped accepting all mail to Canada June 17, on the expectation that the labor dispute between Canada Post and its workers will last at least into the week of June 20. In a statement, the USPS said it would "suspend accepting mail destined to Canada" starting June 18. "As a convenience to our customers and to minimize service disruptions, we arranged to accept mail destined for Canada as long as possible," the USPS vice president said. Source: http://www.vancouversun.com/news/postal+service+shuts+door+mail+Canada/4967912/story.html

PUBLIC HEALTH

Germany: E. coli epidemic united 2 deadly traits. The German E. coli epidemic was more deadly than previous outbreaks because it combined dangerous characteristics of two different strains of the bacteria, researchers said June 23. U.S. health officials said the death of an Arizona man may be linked to the outbreak. The bacteria produced a poisonous byproduct called Shiga toxin, and had the ability to stack together and stick to the gut, researchers led by the director of the Hygiene Institute at the University of Muenster said in an article published online June 23 in the Lancet Infectious Diseases journal. The team found both characteristics in all 80 patients they tested. The unusual combination of traits made it more likely for infected people to develop a potentially fatal kidney complication called hemolytic uremic syndrome, or HUS, the researchers said. As of June 22, the outbreak had sickened 3,601 people, including 815 with HUS, and killed 39, according to the Robert Koch Institute. About 1,000 Shiga toxin-producing E. coli infections and 60 HUS cases typically occur in Germany each year, the researchers said. An Arizona resident who died in mid-June may be the first U.S. death from the outbreak. The man, who was older than 65, recently had visited Germany, according to Arizona health officials. He experienced a high fever shortly after returning to the United States, and suffered from the same type of kidney failure associated with the European strain of E. coli, an Arizona health department epidemiologist, said. Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/06/23/MNEH1K1UN4.DTL

FBI 'seeing a trend' in surgical-instrument theft. The theft of surgical instruments at the Montreal General and Montreal Children's hospitals in Canada in the past 6 months are not rare incidents, but part of a "major problem" plaguing healthcare establishments across North America for years, experts said. An international black market in stolen surgical instruments and equipment is thriving — in part, because law-enforcement agencies are not taking the problem seriously enough, suggests a former police detective who investigated the theft of high-priced

endoscopes in Chicago, Illinois. In the United States, numerous hospitals have been targeted by employees or thieves posing as sales representatives for companies that sell the equipment, said a spokesman who used to work as a detective with the Veterans Administration Police in Chicago. In England, National Health Service officials suspect criminal gangs have been stealing expensive diagnostic equipment — including endoscopes — for sale on the black market in eastern Europe and Africa. In Montreal, thieves have stolen several sets of surgical instruments worth tens of thousands of dollars from the Montreal General and Montreal Children's hospitals since November. The surgical kits are used in orthopedic and trauma surgery. Source: http://www.montrealgazette.com/health/seeing+trend+surgical+instrument+theft/4978502/story.html

UN: Cancer, diabetes kill millions, cost trillions globally. Nearly two-thirds of deaths in the world are caused by noncommunicable diseases such as cancer, diabetes, and heart and lung disease which are rapidly increasing at a cost to the global economy of trillions of dollars, according to U.N. estimates, and preliminary results of a new study. The secretary-general said in a report circulated June 20 that while the international community has focused on communicable diseases such as HIV/AIDS, malaria, and tuberculosis, the four main noncommunicable diseases "have emerged relatively unnoticed in the developing world and are now becoming a global epidemic." According to the report, 36 million people died from noncommunicable diseases in 2008, representing 63 percent of the 57 million global deaths that year. Nearly 80 percent of deaths from these diseases were in the developing world, and 9 million deaths were of men and women under the age of 60, it said. In 2030, the report said, these diseases are projected to claim the lives of 52 million people. Both the human and economic burden of noncommunicable diseases can be contained, he said, by devoting resources directly or indirectly to prevention, screening, and treatment throughout the world. Source: http://www.msnbc.msn.com/id/43473027/ns/health-diabetes/

TRANSPORTATION

(Alaska) **Mudslides close portion of Taylor Highway.** Numerous mudslides in Alaska have blocked a portion of the Taylor Highway, and part of the Steese Highway was closed June 23. The Fairbanks Daily News-Miner reported the highway was blocked June 23 from Mile 114 to Mile 116. The Alaska Department of Transportation said personnel are working to remove the slides. The remainder of the Taylor Highway was open June 23, as was the Top of the World Highway. But transportation officials were urging motorists to drive slowly. Officials also said the Steese Highway outside Circle was closed because of heavy rain and flooding. Many areas of the road between Mile 152 to Mile 158 were washed out. Officials said the road was impassable. Crews were slated to start working on the road June 24. Source: http://www.adn.com/2011/06/23/1933231/mudslides-close-portion-of-taylor.html

Minister cites likely pilot error in Russian plane crash that kills 44. Officials are searching for answers after a Russian jetliner made a premature descent and burst into flames in the country's northwest, killing 44 people and injuring 8 others June 21. "I do not want to prejudge

the investigation and all that, but preliminary information suggests an obvious pilot error in poor weather conditions," the Russian Deputy Prime Minister said, according to the state-run RIA-Novosti news service. Investigators recovered the flight data recorder and cockpit voice recorder from the site of the crash, the investigative committee probing the crash said. The cause of the premature descent will be investigated by the Inter-State Aviation Committee, and the so-called black boxes will be recovered and sent to Moscow for deciphering, the Russian deputy transport minister said on Russian state tv. The dead included 36 Russians, 4 people with joint U.S.-Russian citizenship, a Swede, a Dutchman, and 2 Ukrainians, according to the transport ministry. Of the injured, five are in critical condition, regional authorities in Petrozavodsk said. Some of the injured were to be transported to Moscow for treatment. The jet with 43 passengers and a crew of 9 took off at night June 20 from Moscow for Petrozavodsk, about 600 miles to the north. Controllers lost contact with the twin-engine Tupolev-134 about 11:40 p.m., and it crashed onto a highway outside Besovets, near the Petrozavodsk airport, the ministry reported. Source: http://www.cnn.com/2011/WORLD/europe/06/21/russia.plane.crash/index.html?hpt=hp_t2

Water and Dams

Nothing significant to Report

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168